

WHAT IS CLAIMED IS:

- 1 1. A method for rapid intrusion detection for network communication
2 comprising the steps of:
3 receiving packets of network data in a network processor coupled to a network
4 fabric;
5 forwarding routed network data to the network fabric; and
6 coupling selected data from the network data to a parallel pattern detection
7 engine (PPDE), for comparing the selected data in parallel to M sequences of pattern
8 data stored in the PPDE and generating a match output signal when at least one of the
9 M sequences of pattern data compares to a portion of the selected data.

- 1 2. The method of claim 1, further comprising the steps of:
2 storing N intrusion signatures in the M PUs sequences of pattern data with
3 corresponding identification (ID) data used to identify which of the N intrusion
4 signatures is detected; and
5 storing action code indicating action to take in response to detecting a
6 particular one of the N intrusion signatures.

- 1 3. The method of claim 2, further comprising the steps of:
2 analyzing the packets of network data for validity thereby generating valid
3 packets of network data as the selected data;
4 comparing the selected data to the store N intrusion signatures and generating,
5 at network data speed, a pattern compare signal and particular ID data when a
6 particular one of the N intrusion signatures is detected; and
7 executing the action code corresponding to the particular one of the N
8 intrusion signatures detected.

1 4. The method of claim 3, wherein the PPDE comprises:
2 an input/output (I/O) interface for coupling data into and out of the PPDE;
3 M' processing units (PUs), each of the M PUs having compare circuitry for
4 comparing each of the sequence of input data to pattern data stored in each of the M
5 PUs and generating a compare output, wherein an address pointer selecting the
6 pattern data in each of the M PUs is modified in response to a logic state of the
7 compare output and an operation code stored with the pattern data;
8 an input bus for coupling the sequence of input data to each of the M PUs in
9 parallel;
10 an output bus coupled to the I/O interface for sending output data to the I/O
11 interface;
12 control circuitry coupled to the I/O interface and coupling control data on a
13 control data bus and identification (ID) on an ID bus to each of the M processing
14 units; and
15 ID selection circuitry for selecting a match ID from ID data identifying the M
16 PUs in response to a pattern match signal and match mode data, wherein the match ID
17 and match data corresponding to the match ID are saved in a temporary register as the
18 output data.

1 5. The method of claim 3, wherein the PPDE further comprises cascade circuitry
2 coupled from each of the M PUs to one or more adjacent PUs within the M PUs for
3 selectively coupling chain data between one or more groups of two or more adjacent
4 PUs selected from the M PUs in response to the control data.

1 6. A system for rapid intrusion detection for a network communication
2 comprising:

3 a network processor;

4 circuitry in the network processor for receiving network data from a network
5 fabric;

6 circuitry in the network processor in the network processor for forwarding
7 routed network data to the network fabric; and

8 circuitry for coupling the network processor to a parallel pattern detection
9 engine (PPDE) for comparing in parallel selected data from the network data to M
10 sequences of pattern data stored in the PPDE and generating a match output signal
11 when at least one of the M sequences of pattern data compares to a portion of the
12 selected data.

1 7. The system of claim 6 further comprising circuitry for storing N intrusion
2 signatures in the M PUs sequence of pattern data with corresponding identification
3 (ID) data used to identify which of the N intrusion signatures is detected.

1 8. The system of claim 6 further comprising circuitry for storing action code
2 indicating action to take in response to detecting a particular one of the N intrusion
3 signatures.

1 9. The system of claim 6, further comprising:

2 circuitry for receiving packets of network data from the network fabric in the
3 network process;

4 circuitry for analyzing the packets of network data for validity generating
5 valid packets of network data;

6 circuitry for forwarding network data from the valid packets of network data
7 to the PPDE,

8 circuitry for comparing the selected data to the store N intrusion signatures
9 and generating, at network data speed, a pattern compare signal and particular ID data
10 when a particular one of the N intrusion signatures is detected; and

11 circuitry for executing the action code corresponding to the particular one of
12 the N intrusion signatures detected.

1 10. The system of claim 9, wherein the PPDE comprises:

2 an input/output (I/O) interface for coupling data into and out of the PPDE;

3 M processing units (PUs), each of the M PUs having compare circuitry for
4 comparing each of the sequence of input data to a pattern data stored in each of the M
5 PUs and generating a compare output, wherein an address pointer selecting the
6 pattern byte in each of the M PUs is modified in response to a logic state of the
7 compare output and an operation code stored with the pattern data ;

8 an input bus for coupling the sequence of input data to each of the M PUs in
9 parallel;

10 an output bus coupled to the I/O interface for sending output data to the I/O
11 interface;

12 control circuitry coupled to the I/O interface and coupling control data on a
13 control data bus and identification (ID) on an ID bus to each of the M PUs; and

14 ID selection circuitry for selecting a match ID from ID data identifying the M
15 PUs in response to a pattern match signal and match mode data, wherein the match ID
16 and match data corresponding to the match ID are saved in a temporary register as the
17 output data.

1 11. The system of claim 10, further comprising cascade circuitry coupled from
2 each of the M PUs to one or more adjacent PUs within the M PUs for selectively

3 coupling chain data between one or more groups of two or more adjacent PUs
4 selected from the M PUs in response to the control data.

1 12. The system of claim 11, wherein the PPDE further comprises an input buffer
2 coupled to the I/O interface for receiving and writing input data as parallel data at a
3 write address.

1 13. The system of claim 12, wherein the PPDE further comprises a multiplexer
2 coupled to the input bus and the input buffer for sequentially coupling single data
3 from the input buffer data to the input bus, wherein parallel data are selected using a
4 read address.

1 14. The system of claim 13, wherein the PPDE further comprises an output buffer
2 coupled to the output bus and to the temporary register for receiving and writing
3 output data to the output buffer at a write address and coupling output data to the
4 output bus corresponding to a read address.

1 15. The system of claim 10, wherein each of M PUs has an ID register for storing
2 a unique ID sent from the control circuitry.

1 16. The system of claim 10, wherein each of M PUs has a control register for
2 storing the match mode data, wherein the match mode data determines criteria for
3 generating the match signal and the match data.

1 17. The system of claim 10, wherein each of the M PUs has a memory register
2 array for storing a sequence of the pattern data and corresponding operation codes
3 addressed by an address register indexed by the address pointer.

1 18. The system of claim 11, wherein the cascade circuitry enables the stored
2 patterns of two or more M PUs to be chained together as a single pattern using the
3 chain data.

1 19. The system of claim 18, wherein the chain data inhibits indexing the pointer
2 of one PU until an adjacent PU coupled with the cascade circuitry has compared a last
3 pattern data to input data.

1 20. The system of claim 10, wherein the compare circuitry in each of the M PUs
2 completes a compare of input data to selected pattern data and generates a compare
3 output and modifies the address pointer in the same cycle of a clock signal.

1

1 21. An intrusion detection system comprising;
2 a network processor having an input connection to a network fabric and an
3 output connection to the network fabric; and
4 a parallel pattern detection engine (PPDE) coupled to the network processor,
5 the PPDE for comparing selected from the network data, in parallel, to M sequences
6 of intrusion signature data corresponding to M intrusion signatures stored in the
7 PPDE and generating a match output signal when one of the M intrusion signatures is
8 detected within the network data, wherein the network processor receives network
9 input data, processes the network input data for forwarding as valid network output
10 data, and couples the valid network output data to the PPDE for real-time detection of
11 intrusion patterns within the valid network output data.